IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA,

Plaintiff,

v.

TIMMY J. REICHLING,

Defendant.

REPORT AND RECOMMENDATION

13-cr-126-bbc

REPORT

On October 13, 2013, a grand jury charged defendant Timmy J. Reichling with two counts of causing the production of child pornography, one count of receiving child pornography, and one count of possessing child pornography. *See* dkt. 1. Reichling has moved to suppress the evidence discovered during the August 22, 2013 execution of two state court search warrants because the warrants lacked probable cause and cast too wide a net. *See* dkt. 10.

The challenged warrant applications are remarkably terse in sections, so that some of Reichling's challenges have traction. From the court's perspective, the pivotal question seems to be whether it was appropriate for the state court to draw the inferences necessary to justify issuing such broadly-encompassing search warrants. Logical arguments can be propounded in both directions; as set forth below, I conclude that suppression is not appropriate and I am recommending that this court deny Reichling's motion.

The Warrant Applications

On May 20, 2013, Sergeant Tony Ruesga, Jr., of the Darlington, Wisconsin Police Department, then a 12-year veteran of the department, submitted to the Circuit Court for

Lafayette County[1] under one case number two search warrant applications. Ruesga sought warrants to search the premises (including outbuildings, vehicles, people present, *etc.*) owned by Reisling's parents at 14265 County Road F in Darlington, and the premises owned by Reisling's brother at 14335 County Road F, particularly a trailer at the end of the drive. The court issued both warrants that same day. Reichling has attached both applications and warrants to his motion, *see* dkt. 10-1. These documents speak for themselves but I will synopsize them in this report for ease of reference.

Each warrant application is identical but for the listing and description of the premises to be searched. At the beginning of his applications, Sgt. Ruesga sets forth seven numbered paragraphs detailing "certain property" that he expects to be present on the premises (which I parse briefly):

1. Images depicting or representing "the possible exploitation, sexual assault and/or enticement of children."

2. Documents evidencing the same thing.

3. All computers and hardware devices, including desktops, laptops, handhelds, tablets, PDAs, cell phones, digital game consoles, audio recorders, video recorders, and any sort of camera.

4. Internal and peripheral digital/electronic storage devices, of any and every type, (most of which are listed).

5. Routers, modems and network equipment used to connect computers to the internet.

6. All user manuals, installation disks *etc.*.

7. Anything displaying or containing passwords, access codes, *etc.*.

[1] According to en.wikipedia.org (accessed on February 17, 2014), in 2010 Lafayette County had a population of about 16,836; Darlington was the county's biggest municipality with a population of 2451.

Sgt. Ruesga does not provide any explanation, either boilerplate or tailored, in which he ties these seven categories of items to his investigation.

As probable cause for the two requested searches, Sgt. Ruesga avers that in July 2010, a 14 year old girl (the victim) "started an online Facebook relationship with a person she only knew as 'Nathan Solman.'" Solman knew how old the victim was, and the victim believed that Solman was a boy her age. Within six weeks, at Solman's request, the victim began sending Solman naked pictures of herself "via picture messages from her cell phone." Between August 2010 and July 2012, the victim sent Solman over 300 naked pictures of herself in various sexual positions. At that point, the victim expressed her intent to stop sending naked pictures to Solman, which caused him to threaten to show to other people the pictures she already had sent unless she continued to send Solman more pictures of herself naked.

In July 2012 the victim agreed to meet Solman in person for the first time. They met in the backyard of the victim's residence. The victim described Solman as a short, stocky white male about 30 years old with curly hair and a straggly beard. The meeting was brief because Solman left in a hurry when the victim's stepfather came outside.

On March 8, 2013 and April 13, 2013, the victim received threatening and stalking text messages from telephone number 608-726-0714. One of the messages sent to the victim from this telephone was "Miss me babi im not going anywhere". The victim presumed it was Solman. The victim texted the sender and asked him to stop; the texted reply on April 30, 2013 was "HaHa". After the victim again texted a request to stop, the sender apparently went silent until June 11, 2013, when the victim received a text message suggesting that the sender currently was watching her while she lounged at a swimming pool. Sgt. Ruesga's affidavit implies that the

victim previously had contacted the police about Solman, although he does not say so; in any event, promptly after the June 11, 2013 text, the victim promptly called Sgt. Ruesga to report what was happening. Sgt. Ruesga directed the victim to text back to the sender and ask where he was. She did so; the sender replied that he suspected the police were watching him now, then taunted the victim. The victim and the sender exchanged a few more creepy emails involving an unshared secret and the victim's boyfriend; the sender did not contact the victim again.

Sgt. Ruesga then outlines the investigatory steps he had taken to identify and locate "Nathan Solman": First, the account for the cell telephone from which the victim had received threatening text messages identified the account holder as Timmy J. Reichling with a Darlington zip code but no street address; the account listed as a secondary number the telephone number of Reichling's parents, who lived at 14265 Country Road F in Darlington. This telephone had been active since December 26, 2009. Second, Sgt. Ruesga obtained from Facebook the internet protocol (IP) address of "Nathan Solman," then learned from Century Link (presumably the internet service provider, or "ISP," although this is not stated) that this IP address was associated with the address at which Reichling's parents lived, 14265 County Road F, Darlington. Third, according to Sgt. Ruesga, the victim's physical description of the man claiming to be Nathan Solman who came to her back yard "resembled" Reichling's description (who actually was 46 years old). Fourth, Sgt. Ruesga learned that Reichling had been convicted in 1993 of repeatedly sexually assaulting a 17 year old girl while threatening her with a knife. Fifth, although Reichling's prison term and probation both had expired, Reichling was a registered sex offender with a listed address at his parents' residence at 14265 County Road F, Darlington. Sixth, the U.S. Postal Service confirmed that Reichling currently was receiving his mail at that address.

Seventh, a confidential informant advised Sgt. Ruesga that Reichling also might be living in a trailer parked on the property owned by Reichling's brother at 14335 County Road F: the CI had seen Reichling exiting the trailer on August 19, 2013, and Sgt. Ruesga had seen photographs of motor vehicles currently or previously registered to Reichling parked outside the trailer. (Sgt. Ruesga had confirmed through a record check that Reichling was a validly-licensed driver in the State of Wisconsin, with two currently-registered vehicles).

Sgt. Ruesga closes by asserting that the information contained in his application gives him reason to believe that Reichling is the person who has been harassing, stalking and enticing the victim, and that physical evidence of these crimes will be found at the two premises for which Sgt. Ruesga is seeking search warrants.

Sgt. Ruesga does not include in his warrant applications any boilerplate explanations of the "whats," "hows," and "whys" of Facebook, IP addresses, ISPs, electronically stored information (ESI), ESI storage media, or the characteristics and techniques of people who troll for child pornography online.

Analysis

Reichling breaks his arguments for suppression into five components: (1) Sgt. Ruesga's search warrant applications do not provide probable cause to believe that Reichling is "Nathan Solman;" (2) The applications fail to allege the source of the allegations about the threatening and harassing phone calls; (3) At most, the application establishes probable cause to seize one cell phone; (4) The mention of "Facebook" does not establish probable cause to seize and search computers or peripherals; and (5) The good faith doctrine of *United States v. Leon*, 468 U.S. 897

(1984) cannot save these warrants. The government disputes Reichling's contentions, asserting that the search warrant is valid, and if it isn't, then the evidence seized is admissible pursuant to the good faith doctrine.

Both sides acknowledge that "a determination of probable cause should be paid great deference by reviewing courts," which are to ensure simply that the issuing court "had a substantial basis for concluding that probable cause existed." *United States v. Scott*, 731 F.3d 659, 665 (7th Cir. 2013), citations omitted. Probable cause is a fluid concept that turns on assessment of probabilities in particular factual contexts; it is established when, based on the totality of circumstances, the application sets forth sufficient evidence to induce a reasonably prudent person to believe that a search will uncover evidence of a crime. *Id.* In issuing a search warrant, the court is given license to draw reasonable inferences concerning where evidence referred to in the affidavit is likely to be kept, taking into account the nature of the evidence and the offense. *Id., quoting United States v. Singleton*, 125 F.3d 1097, 1102 (7th Cir. 1997). To the same effect, officers reporting what their investigation has uncovered are entitled reasonably to rely on their special knowledge to assess probabilities and draw inferences; the issuing court then may take into account the experience and special knowledge of the officers if the search warrant explains the significance of specific types of information. *Id.*, citations omitted.

Further, and more critically to this case, while it may be "prudent" for the officer seeking a warrant to apprise the issuing judge of the way computers work–for instance, that files deleted from are recoverable–this sort of explanation "shouldn't be required to make the warrant valid; it is or should be common knowledge." *United States v. Seiver*, 692 F.3d 774, 777-78 (7th Cir. 2012). In *Seiver*, the court criticizes eight appellate opinions from six circuits (including two

from the Seventh) for laboring under a misapprehension about the way computers store information that "reflects a misunderstanding of computer technology." *Id.* at 775-76. The court (by Judge Posner) then provides its own primer on the relevant technology (apparently from Judge Posner's own knowledge and research as opposed to anything contained in the search warrant that the defendant/appellant was challenging on appeal).

The court's observations in *Seiver* are important in this case because Sgt. Ruesga did not explain in his affidavit why the digital photographs that the victim took with and sent from her cell phone might be found on or in the items and devices listed in numbered paragraphs 3 and 4 of Sgt. Ruesga's items-to-be-seized list, namely computers, hardware devices, desktops, laptops, handhelds, tablets, PDAs, cell phones, digital game consoles, or internal and peripheral digital/electronic storage devices. Contrast Sgt. Ruesga's silence with this paragraph provided by the applicant for a child pornography search warrant challenged in *United States v. Carroll*, 2013 WL 937832 (S.D. Ind. 2013):

> With today's technology, images may be copied with the touch of a button. Memory sticks, sims cards and other storage devices now allow users to simply move the images from one device or storage area to another with great ease and speed. This allows for images to be placed on multiple devices with a house. These devices are not only used to copy and move images, but they offer great storage capabilities as well. They provide a highly mobile source of storage which can easily be removed from the computer device and hidden.
>
> *Id.* at *5.

This paragraph (submitted by a detective in the Indianapolis Police Department) succinctly explains why there would be probable cause to search all electronic devices used or possessed by a person to whom digital photographs of child pornography had been send from a cell phone.

If Sgt. Ruesga had included a similar paragraph in his affidavits to the state court, adding a sentence identifying Facebook as a program through which parties often communicate and share photographs, then many Reichling's arguments for suppression would evanesce.

But Sgt. Ruesga's failure to include such information in his application ought not result in suppression because everything stated in the above-quoted paragraph from *Carroll* qualifies as common knowledge. Certainly, new and unfamiliar technology must be explained in a search warrant affidavit in order to ensure that the court understands the evidence and can draw accurate and appropriate inferences and conclusions; but over time, that technology becomes old and familiar. Cell phones have been used to take photographs since the mid-1990s.[2] Cell phone cameras are routinely and commonly used by grade-schoolers[3] to grandparents[4] to take selfies that they post by the billions on Facebook[5] and send to their friends to share, sort and store as they choose, on their own phones, their tablets, flash drives, whatever.

This technology and these practices are so longstanding, so well-understood and so commonplace that in May, 2013, Sgt. Ruesga was not *required* to explain this in his warrant applications to make the subsequently-issued warrants valid. It would have been prudent–and preferable–for Sgt. Ruesga to have included in his applications a paragraph like that provided in

---

[2] According to Wikipedia, the first known publically shared photograph via a cell phone occurred sixteen years before Sgt. Ruesga applied for his warrant, on June 11, 1997 when Phillip Kahn wirelessly transmitted maternity ward photos of his daughter to two thousand friends and family members. *See* http://en.wikipedia.org/wiki/camera_phone, accessed February 25, 2014.

[3] A Google search of "elementary school cell phone policy" produced over 4 million results.

[4] A Google search of "cell phones for senior citizens" produced over 1 million results.

[5] According to Wikipedia, as of February 2011, Facebook had become the largest online photohost, with an estimated 100 billion photos; as of October 2011, over 350 million users accessed Facebook through their mobile phones, accounting for 33% of all Facebook traffic. *See* http://en.wikipedia.org/wiki/History_of_Facebook`, accessed February 25, 2014.

Carroll, but it was not improper for the state court to issue the requested warrants without it. This is because, as noted above, in issuing these search warrants, the state court had license to draw reasonable inferences concerning where evidence referred to in the affidavits was likely to be kept, taking into account the nature of the evidence and the offense. There can be no serious doubt that the judge who issued these two warrants would have been sufficiently familiar with the applicable technology and how people routinely used it to approve Sgt. Ruesga's request to seize and search the computers, hardware devices, desktops, laptops, handhelds, tablets, PDAs, cell phones, digital game consoles, and internal and peripheral digital/electronic storage devices found at the two named premises.[6] Accordingly, I am recommending that this court reject Reichling's multi-part argument that there was no probable cause to seize and then search computers and other ESI storage devices at the two targeted premises.

Sgt. Ruesga's laconic and poorly-worded affidavits present other problems that Reichling cites as grounds to quash the warrants. Reichling argues that the affidavits do not provide probable cause to believe that he is "Nathan Solman." Reichling identifies, then challenges the two alleged evidentiary links in the affidavits: first, that the IP address associated with 14265 County Road F (Reichling's parents address, where he was living) had been identified as "associated" with the Facebook account for Nathan Solman; second, the victim's description of Nathan Solman "resembles" Reichling.

---

[6] If the victim had made hard copies of the photographs and mailed them to Nathan Solman, no one would contend that it was necessary for Sgt. Ruesga to explain in his application to the court that printed photographs of naked teenagers can be stored not just in photo albums, but also in mislabeled file folders, at the bottom of a sock drawer in the dresser, in a shoe box under a bed, between the pages of books or magazines on the coffee table, in a cereal box in the pantry, *etc.*, in order for the court to authorize the search of every location in which such a photograph might be found on the premises. The same logic should apply to digitally conveyed photographs.

Dealing with the second point first, Reichling correctly points out that Sgt. Ruesga doesn't provide a basis for how he knows this. Reichling acknowledges that what little boilerplate Sgt. Ruesga included in his application says that Sgt. Ruesga generated information "through personal investigation, personal observation, and review of the official reports and records of the Darlington Police Department"; Reichling characterizes this statement as so vague as to be meaningless. Brief in Support, dkt. 16, at 7. Reichling also points out that the victim's estimate of "Nathan Solman"'s age was about 15 years younger than Reichling.

The government responds that because Sgt. Ruesga reported that he conducted record checks to determine that Reichling was a registered driver in the State of Wisconsin and was a registered sex offender; "common sense dictates that during these searches and this investigation, Sergeant Ruesga became familiar with Timmy Reichling's appearance." Gov't. Br. in Opp., dkt. 18, at 4, n. 2. Here again, Sgt. Ruesga should have–and easily could have–provided the missing evidentiary link on the identity issue. The question before this court is whether the state court had a substantial basis to conclude that Sgt. Ruesga's assertion of a "resemblance" was worthy of credence. Put another way, was this a reasonable inference for the court to draw from the record? As the government points out, it is common knowledge that driver license information includes physical descriptors and usually a photograph. (Sex registry information probably contains similar information, but I don't know this, I don't know if the state court judge knew this and the contents of sex registries are not common knowledge, so this data source must be deemed speculative). However, Sgt. Ruesga's review of Wisconsin DOT records provides an adequate basis to allow the state court to accept his report that the victim's description of

Nathan Solman resembled Reichling. The victim's fifteen-year mistake on age seems inconsequential; is any young teenager capable of accurately judging the age of anyone over 30?

In any event, this all gets pulled into sharper focus due to Sgt. Ruesga's report that the physical address "associated with" Nathan Solman's Facebook account was the residence where Reichling–who had been convicted of sexually assaulting a teenage girl–currently was living, 14265 County Highway F, Darlington. Reichling takes issue with Sgt. Ruesga's word choice and foundational explanation of this connection, complaining that it is all too vague to merit credence by the state court. The government concedes that Sgt. Ruesga "was not as articulate as [he] could be," but that he was clear enough for the state court to have concluded that whoever was using the Solman Facebook page was connected to the residence at 14265 County Road F. The government is correct. The most natural reading of Sgt. Ruesga's application–and the most reasonable conclusion to draw from it–is that the person using the Solman Facebook page is using it at this residence.

The evidentiary bricks stack up with increasing speed: 14265 County Road F was Reichling's current address. Reichling had bought the telephone that sent threatening text messages to the victim. Reichling was still listed as the customer for that telephone and TracFone information listed as a secondary number for this account the telephone at 14265 County Road F. One of the messages sent from this phone was "Miss me babi im not going anywhere". The common denominator here, the overlap of the Venn circles, was Reichling.

As the Court noted 65 years ago in *Brinegar v. United States*, 338 U.S. 160, 175 (1949),

> In dealing with probable cause, . . . as the very name implies, we are dealing with probabilities. These are not technical; they are the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians act.

This is a low evidentiary threshold, requiring only a probability or a substantial chance of criminal activity, not an actual showing of such activity. *United States v. Roth*, 201 F.3d 888, 893 (7th Cir. 2000), *quoting Illinois v. Gates*, 462 U.S. 213, 244 (1983). This standard has been met here. Taking a practical view of the totality of the circumstances–including both the gaps in Sgt. Ruesga's affidavits and the inferences that the issuing court reasonably could draw–the two applications provide sufficient evidence to induce a reasonably prudent person to believe that Reichling was the person who had inveigled the victim to send him photographs, the person she met in her backyard, and the person who stalked and taunted her with text messages. There was substantial evidence supporting the state court's conclusion that evidence of child pornography would be found where Reichling resided. This then brings into the mix the evidence establishing the Reichling also might be living in the trailer located at 14335 County Road F.

At this juncture in the analysis, there is a fork in the road: either this court endorses or rejects the state court's authorization to search all of the computers and storage devices or it doesn't. Given the all↔nothing dichotomy presented, it would seem that *Leon's* good faith doctrine does not apply. Under *Leon*, even if a search warrant is invalid because the supporting affidavit failed to establish probable cause, evidence seized in executing the warrant should not be suppressed if the officers relied in good faith on the judge's decision to issue the warrant. *See United States v. Miller*, 673 F.3d 688, 693 (7th Cir. 2012). A defendant can defeat the good faith exception by showing: (1) the issuing judge abandoned his/her detached and neutral judicial role; (2) the office was dishonest or reckless in preparing the affidavit; or (3) the warrant was so lacking in probable cause that the officer could not reasonably rely on the judge's issuance of it.

Id. In the instant case, Sgt. Ruesga did not provide any information in his affidavit that would have justified searching for the victim's photographs on computers and other ESI storage media located at the premises to be searched. Unless this court determines that it is common knowledge that digital photographs can be and routinely are stored on other electronic devices, then there would be no basis for the court to have authorized their search and no basis for Sgt. Ruesga reasonably to rely on the court's issuance of a warrant to seize and search such devices. As noted above, I am recommending that the court accept this information as common knowledge.

If the court does not accept this information as common knowledge, then Reichling would seem to be entitled to suppression of any information retrieved from any ESI storage device except for his own cell phone and perhaps his Facebook page and account. Reichling essentially concedes the search of his telephone (if the court rejects his other arguments) but contends that Sgt. Ruesga did not adequately connect the evidentiary dots between the victim's cell phone photos and "Nathan Solman"'s Facebook account. The government has the better argument here: the victim specifically reported that she was engaged in a Facebook relationship with "Solman." There is no mention of phone-to-phone communication during the period the victim was sending Solman digital photographs. The clear implication of Sgt. Ruesga's affidavit is that the victim was sending her pictures to Solman's Facebook page. However, if the court agrees with Reichling that this is not enough, and that the storage and display of digital photographs on Facebook is not common knowledge, then the court also should suppress any evidence found on Reichling/Solman's Facebook account.

RECOMMENDATION

Pursuant to 42 U.S.C. § 636(b)(1)(B) and for the reasons stated above, I recommend that this court deny defendant Timmy J. Reichling's motion to suppress evidence seized during execution of the two challenged search warrants.

Entered this 28th day of February, 2014.

BY THE COURT:

/s/

STEPHEN L. CROCKER
Magistrate Judge

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WISCONSIN
120 N. Henry Street, Rm. 540
Post Office Box 591
Madison, Wisconsin 53701

Chambers of
STEPHEN L. CROCKER
U.S. Magistrate Judge

Telephone
(608) 264-5153

February 28, 2014

Elizabeth Altman
Assistant United States Attorney
660 West Washington Avenue, Ste. 303
Madison, WI 53703

Robert T. Ruth
Ruth Law Office, S.C.
7 North Pinckney Street, Ste. 240
Madison, WI 53703

Re: United States v. Timmy Reichling
Case No. 13-cr-126-bbc

Dear Counsel:

The attached Report and Recommendation has been filed with the court by the United States Magistrate Judge.

The court will delay consideration of the Report in order to give the parties an opportunity to comment on the magistrate judge's recommendations.

In accordance with the provisions set forth in the memorandum of the Clerk of Court for this district which is also enclosed, objections to any portion of the report may be raised by either party on or before March 14, 2014, by filing a memorandum with the court with a copy to opposing counsel.

If no memorandum is received by March 14, 2014, the court will proceed to consider the magistrate judge's Report and Recommendation.

Sincerely,

/s/

Connie A. Korth
Secretary to Magistrate Judge Crocker

Attachment

MEMORANDUM REGARDING REPORTS AND RECOMMENDATIONS

Pursuant to 28 U.S.C. § 636(b), the district judges of this court have designated the full-time magistrate judge to submit to them proposed findings of fact and recommendations for disposition by the district judges of motions seeking:

(1) injunctive relief;
(2) judgment on the pleadings;
(3) summary judgment;
(4) to dismiss or quash an indictment or information;
(5) to suppress evidence in a criminal case;
(6) to dismiss or to permit maintenance of a class action;
(7) to dismiss for failure to state a claim upon which relief can be granted;
(8) to dismiss actions involuntarily; and
(9) applications for post-trial relief made by individuals convicted of criminal offenses.

Pursuant to § 636(b)(1)(B) and (C), the magistrate judge will conduct any necessary hearings and will file and serve a report and recommendation setting forth his proposed findings of fact and recommended disposition of each motion.

Any party may object to the magistrate judge's findings of fact and recommended disposition by filing and serving written objections not later than the date specified by the court in the report and recommendation. Any written objection must identify specifically all proposed findings of fact and all proposed conclusions of law to which the party objects and must set forth with particularity the bases for these objections. An objecting party shall serve and file a copy of the transcript of those portions of any evidentiary hearing relevant to the proposed findings or conclusions to which that party is objection. Upon a party's showing of good cause, the district judge or magistrate judge may extend the deadline for filing and serving objections.

After the time to object has passed, the clerk of court shall transmit to the district judge the magistrate judge's report and recommendation along with any objections to it.

The district judge shall review de novo those portions of the report and recommendation to which a party objects. The district judge, in his or her discretion, may review portions of the report and recommendation to which there is no objection. The district judge may accept, reject or modify, in whole or in part, the magistrate judge's proposed findings and conclusions. The district judge, in his or her discretion, may conduct a hearing, receive additional evidence, recall witnesses, recommit the matter to the magistrate judge, or make a determination based on the record developed before the magistrate judge.

NOTE WELL: A party's failure to file timely, specific objections to the magistrate's proposed findings of fact and conclusions of law constitutes waiver of that party's right to appeal to the United States Court of Appeals. ***See United States v. Hall,*** **462 F.3d 684, 688 (7th Cir. 2006).**